REMARKS

In the final Office Action,[1] the Examiner rejected claims 9 and 14 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,537,314 to Kanter ("*Kanter*") in view of U.S. Patent 6,594,640 to Postrel ("*Postrel*") and U.S. Patent 6,012,039 to Hoffman et al. ("*Hoffman*"). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

Claim 9, as amended, recites a point transfer dealer system comprising, among other things, "a point redemption system for receiving first data encrypted using a public key of the point redemption system from the customer, the first data comprising second data encrypted using a private key of the customer."

Kanter discloses "a participant's personal security number which can be used to verify against a code" (col. 17, lines 63-64) and "[t]he account number and security codes are examined to . . . verify the participants account . . . and the sponsoring company account having the same numbers and codes" (col. 23, lines 47-51). However, merely using of security number and code in *Kanter* cannot teach or suggest "data encrypted using a . . . key," as recited in claim 9. *Kanter* is completely silent with respect to any encryption or the use of public and private keys for encrypting.

Postrel fails to cure the above-noted deficiencies of *Kanter* at least because *Postrel* is also silent with respect to any encryption or the use of public and private keys for encrypting.

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

Hoffman discloses a "DES encryption algorithm, preferably . . . [employing] successive encrypt/decrypt/encrypt operations using two distinct 56-bit DES keys." *Hoffman*, col. 7, lines 13-16. A Triple DES, using decryption as the middle step, can be represented by $DES(k_3;DES^{-1}(k_2;DES(k_1;M)))$, wherein k_1, k_2, and k_3 are keys and M is the message to be encrypted. Wikipedia, http://en.wikipedia.org/wiki/Triple_DES, as of October 2, 2007 (copy enclosed). Therefore, in *Hoffman*, the same data is encrypted multiple times. However, mere multiple encryption of the same data cannot disclose encrypted data comprising another encrypted data within it. Therefore, the disclosure in *Hoffman* cannot teach or suggest "the [encrypted] first data . . . comprising [encrypted] second data," as recited in claim 9 (emphasis added).

Hoffman further discloses "public/private key system may also be used to encrypt information." *Hoffman*, col. 7, lines 18-19. But again, the mere use of public and private keys in *Hoffman* does not disclose encrypted data comprising another encrypted data within it. Therefore, *Hoffman* also fails to cure the above-noted deficiencies of *Kanter* and *Postrel*.

For at least the reasons give above, the cited references, taken alone or in proper combination, fail to disclose each and every element of claim 9. Therefore, a *prima facie* case of obviousness has not been established with respect to claim 9. In addition, claim 14, although different in scope from claim 9, is also allowable over the cited references for at least reasons similar to those given for claim 9. Accordingly, Applicant respectfully requests the Examiner to reconsider and withdraw the rejection of claims 9 and 14 under 35 U.S.C. § 103(a).

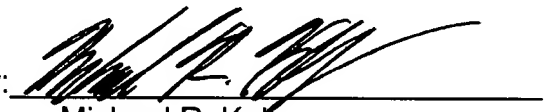
In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 2, 2007

By: 
Michael R. Kelly
Reg. No. 33,921

Attachment: "Triple DES," Wikipedia (2 pages).

Triple DES

From Wikipedia, the free encyclopedia

In cryptography, **Triple DES** is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times.

Contents

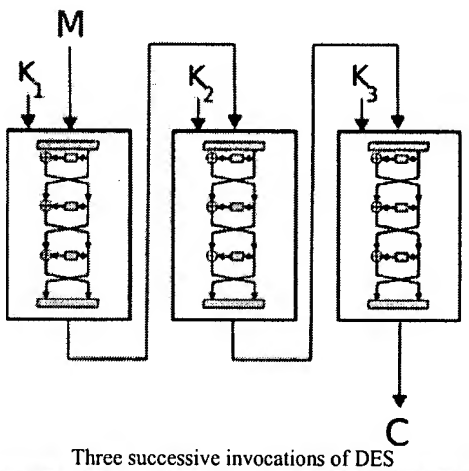
Acronyms

Triple DES is also known as **TDES** or, more standard, **TDEA** (Triple Data Encryption Algorithm [1]). The non-standard convention to use DES (standard) when we actually mean DEA (algorithm) is so widespread that in order to avoid confusion we use it in this article. On the other hand, since there are variations of TDES which use two different keys (**2TDES**) and three different keys (**3TDES**) the non-standard abbreviation **3DES** is confusing and should be avoided.

Algorithm

When it was found that a 56-bit key of DES is not enough to guard against brute force attacks, TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. The use of three steps is essential to prevent meet-in-the-middle attacks that are effective against double DES encryption. Note that DES is not a group; if it were one, the TDES construction would be equivalent to a single DES operation and no more secure.

Triple DES



Three successive invocations of DES

General	
Designer(s):	IBM
First published:	1978
Derived from:	DES
Cipher detail	
Key size(s):	112 (2TDES) or 168 bits (3TDES)
Block size(s):	64 bits
Structure:	Feistel network
Rounds:	48 DES-equivalent rounds
Best public cryptanalysis	

Lucks: 2^{32} known plaintexts, 2^{113} operations including 2^{90} DES encryptions, 2^{88} memory; Biham: find one of 2^{28} target keys with a handful of chosen plaintexts per key and 2^{84} encryptions

The simplest variant of TDES operates as follows: $\mathrm{DES}(k_3;\mathrm{DES}(k_2;\mathrm{DES}(k_1;M)))$, where M is the message block to be encrypted and k_1, k_2, and k_3 are DES keys. This variant is commonly known as EEE because all three DES operations are encryptions. In order to simplify interoperability between DES and TDES the middle step is usually replaced with decryption (EDE mode): $\mathrm{DES}(k_3;\mathrm{DES}^{-1}(k_2;\mathrm{DES}(k_1;M)))$ and so a single DES encryption with key k can be represented as TDES-EDE with $k_1 = k_2 = k_3 = k$. The choice of decryption for the middle step does not affect the security of the algorithm.

Security

In general TDES with three different keys (3TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. A variant, called two-key TDES (2TDES), uses $k_1 = k_3$, thus reducing the key size to 112 bits and the storage length to 128 bits. However, this mode is susceptible to certain chosen-plaintext or known-plaintext attacks [2] [3] and thus it is officially [4] designated to have only 80-bits of security.

As of 2005, the best attack known on 3TDES requires around 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions, and 2^{88} memory[5] (the paper presents other tradeoffs between time and memory). This is not currently practical. If the attacker seeks to discover any one of many cryptographic keys, there is a memory-efficient attack which will discover one of 2^{28} keys, given a handful of chosen plaintexts per key and around 2^{84} encryption operations[6]. This attack is highly parallelizable and verges on the practical, given billion-dollar budgets and years to mount the attack, though the circumstances in which it would be useful are limited.

Usage

TDES is slowly disappearing from use, largely replaced by its natural successor, the Advanced Encryption Standard (AES). One large-scale exception is within the electronic payments industry, which still uses 2TDES extensively and continues to develop and promulgate standards based upon it (e.g. EMV). This guarantees that TDES will remain an active cryptographic standard well into the future.

By design, DES and therefore TDES, suffer from slow performance in software; on modern processors, AES tends to be around six times faster. TDES is better suited to hardware implementations, and indeed where it is still used it tends to be with a hardware implementation (e.g., VPN appliances and the Nextel cellular and data network), but even there AES outperforms it. Finally, AES offers markedly higher security margins: a larger block size, potentially longer keys, and as of 2007, no known public cryptanalytic attacks.

See also

- DES-X
- Walter Tuchman
- Horst Feistel
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

References

1. ^ NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (PDF), Special Publication 800-67.
2. ^ Ralph Merkle, Martin Hellman: On the Security of Multiple Encryption (PDF), Communications of the ACM, Vol 24, No 7, pp 465–467, July 1981.
3. ^ Paul van Oorschot, Michael J. Wiener , *A known-plaintext attack on two-key triple encryption*, EUROCRYPT'90, LNCS 473, 1990, pp 318–325.
4. ^ NIST, Recommendation for Key Management — Part 1: general (PDF), Special Publication 800-57.
5. ^ Stefan Lucks: Attacking Triple Encryption (PDF), Fast Software Encryption 1998, pp 239–253.
6. ^ Eli Biham: How to Forge DES-Encrypted Messages in 2^{28} Steps (PostScript), 1996.

Block ciphers

Algorithms: 3-Way | AES | Akelarre | Anubis | ARIA | BaseKing | Blowfish | C2 | Camellia | CAST-128 | CAST-256 | CIKS-1 | CIPHERUNICORN-A | CIPHERUNICORN-E | CMEA | Cobra | COCONUT98 | Crab | CRYPTON | CS-Cipher | DEAL | DES | DES-X | DFC | E2 | FEAL | FROG | G-DES | GOST | Grand Cru | Hasty Pudding Cipher | Hierocrypt | ICE | IDEA | IDEA NXT | Iraqi | Intel Cascade Cipher | KASUMI | KHAZAD | Khufu and Khafre | KN-Cipher | Libelle | LOKI89/91 | LOKI97 | Lucifer | M6 | MacGuffin | Madryga | MAGENTA | MARS | Mercy | MESH | MISTY1 | MMB | MWA | MULTI2 | NewDES | NOEKEON | NUSH | Q | RC2 | RC5 | RC6 | REDOC | Red Pike | S-1 | SAFER | SC2000 | SEED | Serpent | SHACAL | SHARK | Skipjack | SMS4 | Square | TEA | **Triple DES** | Twofish | UES | Xenon | xmx | XTEA | XXTEA | Zodiac

Design: Feistel network | Key schedule | Product cipher | S-box | SPN

Attacks: Brute force | Linear / Differential / Integral cryptanalysis | Mod *n* | Related-key | Slide | XSL

Standardization: AES process | CRYPTREC | NESSIE

Misc: Avalanche effect | Block size | IV | Key size | Modes of operation | Piling-up lemma | Weak key

Cryptography

History of cryptography | Cryptanalysis | Cryptography portal | Topics in cryptography

Symmetric-key algorithm | Block cipher | Stream cipher | Public-key cryptography | Cryptographic hash function | Message authentication code | Random numbers

Category: Block ciphers